Fo 1/1

PCT/EP 99 / 10141

REC'D 07 FEB 2000

WIPO PCT

09/683325

SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

EP 99/10141

4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

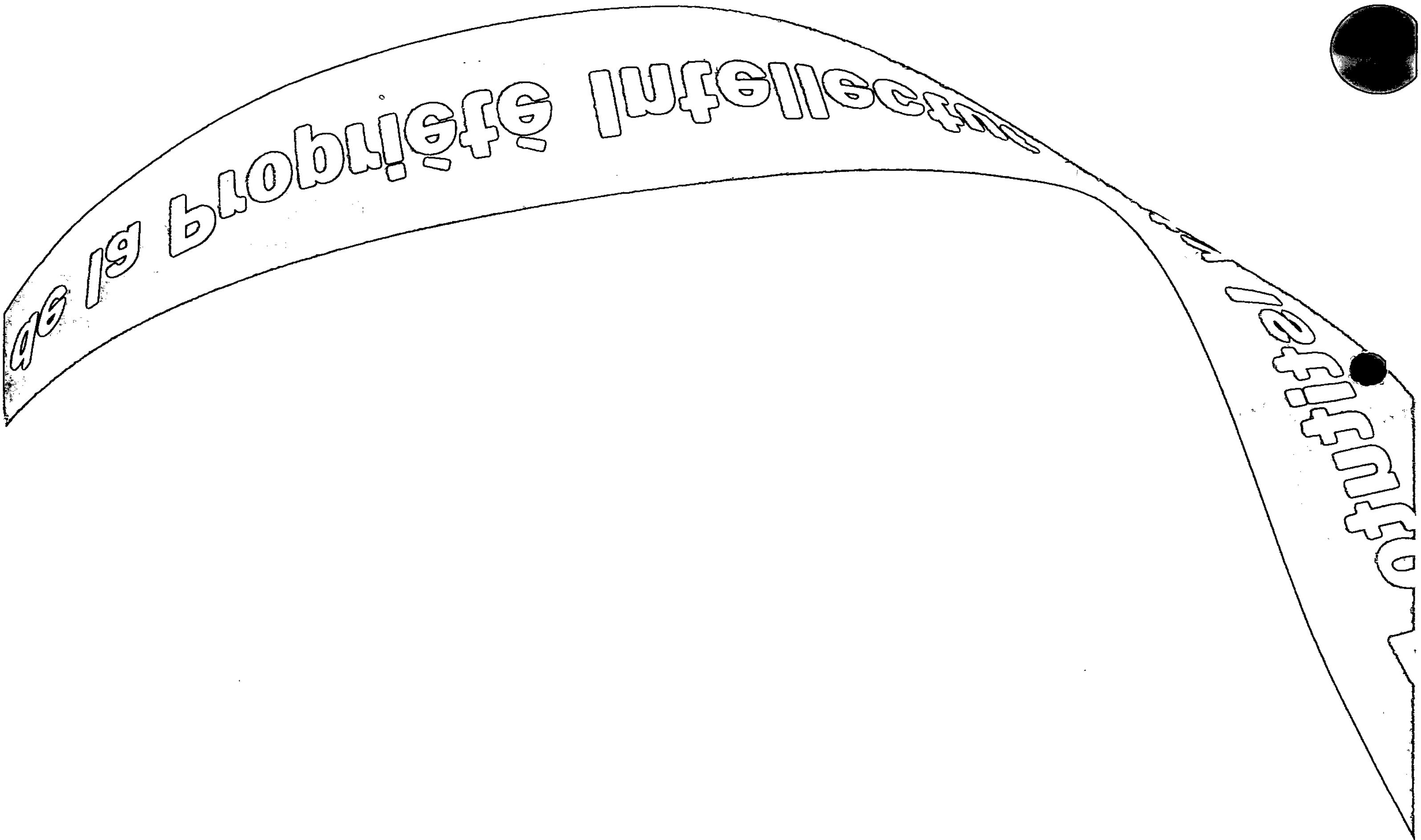
Gli uniti documenti sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territtorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, - 8. Dez. 1999

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione dei brevetti

Rolf Hofstetter



Patentgesuch Nr. 1998 2557/98

HINTERLEGUNGSBESCHEINIGUNG (Art. 46 Abs. 5 PatV)

Das Eidgenössische Institut für Geistiges Eigentum bescheinigt den Eingang des unten näher bezeichneten schweizerischen Patentgesuches.

Titel:
Aktivierbares Dokument und System für aktivierbare Dokumente.

Patentbewerber:
Electrowatt Technology Innovation AG

6301 Zug

Anmeldedatum: 24.12.1998

Voraussichtliche Klassen: G06K

Aktivierbares Dokument und System für aktivierbare Dokumente

Die Erfindung bezieht sich auf ein aktivierbares Dokument gemäss dem Oberbegriff des Anspruchs 1 und auf ein System für aktivierbare Dokumente gemäss dem Oberbegriff des Anspruchs 9.

Solche aktivierbare Dokumente sind für persönliche Ausweise verwendbar, wie z.B. Bankschecks, Pässe, Identitätskarten, Abonnements, Billette, Gesundheitskarten, Kreditkarten, IC-Karten, elektronische Geldbörsen (smart cards), Wertdokumente usw. Ein solches System, das aktivierbare Dokumente verwendet, sind vor allem bei Echtheitskontrollen und/oder Inhaber - Kontrollen der Dokumente verwendbar.

Zur Sicherung der genannten Dokumente werden visuell leicht erkennbare Hologramme und andere Beugungsstrukturen eingesetzt, wobei sie meist in Form von Etiketten aus einem die beugungsoptisch wirksamen Strukturen schützenden Kunststofflaminat mit dem Substrat des Dokuments unlösbar verbunden sind (EP 0 330 738 A1). An und für weisen solche Dokumente einen sehr hohen Sicherheitsstandard gegen Fälschungen oder Verfälschungen auf.

Aus der EP 0 713 197 A1 ist ein Datenträger in Kartenform mit einer in den Kartenkörper integrierten elektronischen Schaltung und einer optischen Markierung bekannt, wobei der Inhalt der elektronischen Schaltung mit der Information der optischen Markierung verknüpft ist. Als optische Markierungen können beispielsweise mit Farbe aufgebrachte Zeichen, wie ein Barcode oder Schriftzeichen, oder beugungsoptisch wirksame Strukturen, wie sie in der CH - PS 653 161 A5, in der EP 0 366 858 A1, in der EP 0 718 795 A1, in der EP 0 883'085 A1 usw. verwendet werden. In den genannten Schriften sind auch Ausführungen von Lese- und Schreibgeräten für die optischen Markierungen beschrieben.

Schliesslich beschreibt die US - PS 3 833 795 die Sicherung der Echtheit von seriell numerierten Dokumenten (Banknoten, Wertpapiere). Eine solches Dokument trägt zwei Nummernfelder, das eine ist für eine fortlaufende Nummerierung der Dokumente, der Identitätsnummer, vorgesehen, das andere ist eine bei der Ausgabe zufällig gewählte Kontrollnummer, die in eine zentral geführte Liste eingetragen wird. Ein ausgegebenes Dokument wird anhand der externen Liste oder mittels eines Listen - Algorithmus überprüft, wobei eine Leseeinrichtung zunächst die Identitätsnummer und die Kontrollnummer abliest und anschliessend die Kontrollnummer der Identitätsnummer auf dem Dokument mit der von der Leseeinrichtung mittels der externen Liste oder des Listen - Algorithmus gefundenen Kontrollnummer vergleicht. Dieses Dokument ist jedoch nicht gegen Kopieren geschützt.

Ein grosses Problem stellt jedoch die Sicherheit der Dokumente im Zeitraum von der Herstellung bis zur Übergabe des Dokuments an die berechtigte Person dar, da in diesem Zeitraum die Dokumente auf dem Transport gestohlen werden können, um mit diesen Dokumenten unberechtigte Personen auszurüsten.

Der Erfindung liegt die Aufgabe zugrunde, ein in grossen Mengen kostengünstig hergestelltes, gegen Kopieren geschütztes Dokument derart zu sichern, dass seine Echtheitsmerkmale erst beim Inverkehrbringen vervollständigt werden und die Echtheitsmerkmale einfach und kostengünstig maschinell zu überprüfen sind.

Die genannte Aufgabe wird erfindungsgemäss durch die im Kennzeichen der Ansprüche 1 und 9 angegebenen Merkmale gelöst. Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Ausführungsbeispiele der Erfindung sind in der Zeichnung dargestellt und werden im folgenden näher beschrieben.

Es zeigen:
- Figur 1 ein Dokument,
- Figur 2 ein aktiviertes Dokument,
- Figur 3 eine IC - Karte als Dokument,
- Figur 4 einen Informationsstreifen,
- Figur 5 ein System,
- Figur 6 ein Validiergerät und
- Figur 7 einen Verifikator.

In der Figur 1 bedeutet 1 ein Dokument, 2 Dokumentennummer, 3 eine optische Markierung, 4 ein Speicherfeld, 5 ein Kontrollfeld und 6 ein Substrat. Das Dokument 1 besitzt ein Substrat 6 aus Papier, Kunststoffvlies, Kunststoffolie, einem Schichtverbund aus Kunststoff, Lacken und/oder Papier usw. Die beiden Oberflächen des Substrats 6 können bedruckt sein, wie dies bei Bankschecks, Pässen, Identitätskarten, Abonnements, Billetts, Gesundheitskarten, Kreditkarten, IC-Karten, elektronische Geldbörsen (smart cards), Wertdokumente, Banknoten usw. üblich ist, und weisen wenigstens auf einer Seite die wenigstens maschinell lesbare Dokumentennummer 2 auf. Die Dokumentennummer 2 kann in Klarschrift und/oder als Strichkode in bekannter Art mit normaler, fluoreszierender oder magnetischer Tinte auf das Substrat 6 aufgebracht sein. Für die optische Markierung 3 sind beispielsweise mit normaler, fluoreszierender oder magnetischer Farbe aufgebrachte oder mittels Perforieren des Substrats 6 erzeugte Zeichen, wie ein Barcode, Schriftzeichen usw., oder beugungsoptisch wirksame Strukturen verwendbar. Die optische Markierung 3 enthält eine digitale Information, eine Kennung 7. Von besonderem Vorteil ist die Verwendung der optischen Markierung 3 mit beugungsoptisch wirksamen Strukturen wegen ihrer hohen Sicherheit gegen Fälschung und Kopieren. Sie sind aus den eingangs genannten Schriften CH 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1 usw. bekannt und eignen sich besonders zum maschinellen Ablesen einer in der beugungsoptischen Markierung 3

enthaltenen Kennung 7. Die Kennung 7 beinhaltet Informationen über die Art des Dokuments, die Dokumentserie usw. nicht aber über die Dokumentennummer 2, die das Dokument 1 innerhalb einer Serie identifiziert, d.h. die Dokumente 1 einer Serie sind kostengünstig herstellbar und unterscheiden sich nur durch die beispielsweise aufgedruckten Dokumentennummern 2. Die Grösse der optischen Markierung 3 ist durch die darin enthaltene Kennung 7 bestimmt und die benötigte Fläche umfasst typisch ungefähr 1 mm^2. Extremwerte für diese Fläche dürften bei 0,1 mm^2 eine untere und bei 1 cm^2 eine obere Grenze erreichen. Die optische Markierung 3 kann auch visuell unsichtbar in einer transparenten Folie gemäss CH 653 161 A5 eingebracht sein oder auch unauffällig innerhalb eines Hologramms oder eines beugungsoptischen Musters, einem Sicherheitsmerkmal 8, beispielsweise gemäss CH 659 433 A5, verborgen sein. Das Sicherheitsmerkmal 8 dient der Identifizierung des Dokuments 1 für den Mann auf der Strasse und wirkt auf dem Dokument 1 sehr auffällig.

Das Speicherfeld 4 und das Kontrollfeld 5 bleiben zur Auslieferung an die Inverkehrbringer (Verkaufsstellen, Ausgabestellen, Bankschalter usw.) leer. Ohne eine in der Figur 2 gezeigte Kontrollnummer 9 im Speicherfeld 4 ist das Dokument 1 unbrauchbar. Beim Inverkehrbringen müssen die Dokumente 1 durch eine Aktivierung ihre Gültigkeit erlangen. Beispielsweise werden die Dokumentennummer 2 und die Kennung 7 maschinell aus dem Dokument 1 abgelesen. Wenigstens diese Informationen werden mit einem ausserhalb des Dokuments vorhandenen ersten geheimen Schlüssel 10 in einer kryptographischen Operation miteinander verknüpft und aus dem Resultat die dem Dokument 1 zugehörige Kontrollnummer 9 erzeugt und in das Speicherfeld 4 eingeschrieben. Das Dokument 1 ist erst jetzt vollständig und seine Gültigkeit ist anhand der Dokumentennummer 2, der Kennung 7 und der Kontrollnummer 9 überprüfbar. Bei bestimmten Dokumentarten ist während der Aktivierung auch die Beschriftung des Kontrollfelds 5 vorgesehen. Der Inhalt des Kontrollfelds 5 umfasst wenigstens visuell lesbare, individuelle, auf eine Person, Veranstaltung, Firma, usw. bezogene Informationen, wie Name, Anschrift, Sozial- oder andere Versicherungsnummer, Staatszugehörigkeit, Zeitangaben, Geldbetrag usw. Diese Informationen, im folgenden Kode 11 genannt, können auch zusammen mit der Dokumentennummer 2, der Kennung 7 mit der kryptographischen Operation zur Kontrollnummer 9 verarbeitet werden.

In einer Ausführung des Dokuments 1 ist nach einem der bekannten Verfahren das Speicherfeld 4 und/oder das Kontrollfeld 5 mit der Kontrollnummer 9 bzw., dem Kode 11 in maschinenlesbarer Druckschrift beschriftet. Diese Klarschrift, z.B. OCR - Schrift, ist sowohl visuell als auch maschinell lesbar. Anstelle oder zusammen mit der Druckschrift kann die Kontrollnummer 9 auch als Strichkode, der im Detailhandel weit verbreitet ist, dargestellt sein.

In der Figur 3 ist eine weitere Ausführung des Dokuments 1 in Form einer Karte (Gesundheitskarte, Kreditkarte, IC-Karte, Smartcards, usw) gezeigt. In das Substrat 6 ist ein an sich bekanntes Modul 12

mit einem der Mikrochip 13 eingelassen, in dessen Speicher 14 das Speicherfeld 4 eingerichtet ist. Das Speicherfeld 4 kann nur einmal mit der Kontrollnummer 9 beim Aktivieren des Dokuments 1 mittels einer über ein Kontaktfeld 15 gesandte elektronischen Signalfolge beschrieben werden, eine spätere Veränderung ist nicht mehr möglich. Wie in der eingangs erwähnten EP 0 713 197 A1 kann die Signalfolge auch mittels hier nicht gezeigten induktiven oder optischen Mitteln an ein entsprechend gestaltetes Modul 12 des Dokuments 1 übertragen werden.

Eine andere Ausführung des Dokuments 1 in Kartenform weist auf dem Substrat 7 einen Magnetstreifen 16 auf. Die Kontrollnummer 9 (Figur 2) und der Kode 11 (Figur 2) wird beim Aktivieren des Dokuments 1 magnetisch kodiert in das Speicherfeld 4 bzw. in das Kodierfeld 5 auf dem Magnetstreifen 16 eingezeichnet. Das Speicherfeld 4 weist nach der Aktivierung im Speicherfeld 4 wenigstens die magnetisch lesbare Kontrollnummer 9 auf.

Eine weitere Ausführung des Dokuments 1 weist im Speicherfeld 4 einen mit dem Substrat 6 während des Herstellungsprozesses des Dokuments 1 aufgebrachten, in der Figur 4 dargestellten beugungsoptischen Informationsträger 17 auf, wie er in der eingangs genannten Schrift EP 0 718 795 A1 beschrieben ist. Der Informationsträger 17 weist im unbeschriebenen Zustand 17' wenigstens eine Reihe von in Paaren 19 angeordneten Beugungsfeldern 18, wobei sich die beiden mikroskopischen Beugungsstrukturen eines Paares 19 in wenigstens einem Gitterparameter unterscheiden. Während des Aktivierens wird die Kontrollnummer 9 als digitale Folge auf dem Informationsträger 17 abgebildet, wobei beim Beschreiben entsprechend dem Bitwert in jedem Paar eines der beiden Beugungsfelder 18 die Beugungsstruktur durch Zuführen von Wärmeenergie zerstört oder die Beugungsstruktur durch Abdecken, z.B. mit einem nicht transparenten Decklack, unwirksam gemacht wird. Im Informationsträger 17'' ist nach der Aktivierung bei jedem Paar eine der beiden Beugungsstrukturen nicht mehr beugungsoptisch wirksam. Das Speicherfeld 4 weist nun die Kontrollnummer 9 in optisch maschinell leicht lesbaren Zeichen auf. Der Vorteil dieses Informationsträgers 17 ist, dass er nur einmal beschrieben werden kann. Jede weitere Veränderung des Informationsträgers 17 ist maschinell leicht zu erkennen.

In einer Ausführung des Dokuments 1 ist die optische Markierung 3 und die Kontrollnummer 9 mit Beugungsstrukturen ausgeführt und auf dem gleichen Informationsträger 17 untergebracht. Der Vorteil dieser Ausführung ist, dass mit einem einzigen optischen Leser 26 gemäss der EP 0 718 795 A1 das Auslesen der Kennung 7 und der Kontrollnummer 9 sowie das Beschriften des Informationsträgers 17 durchgeführt wird. Das teuere Sicherheitsmerkmal 8 (Figur 1) kann weggelassen werden.

Die Beschriftungen 2, 9, 11, das Modul 12 und der Magnetstreifen 16 können an sich beliebig auf den beiden Seiten des Dokuments 1 verteilt sein, wobei üblicherweise nur der Magnetstreifen 16 auf der Rückseite des Substrats 6 angeordnet ist.

Die Figur 5 zeigt ein System 20, das sich für die Verwendung der vorstehend beschriebenen Dokumente 1 eignet. Das System 20 umfasst wenigstens ein Dokument 1, ein Validiergerät 21 für die Aktivierung des Dokuments 1 und einen Verifikator 22, mit dem eine Echtheitskontrolle des Dokuments 1 durchzuführen ist. Während die Validiergeräte 21 bei den wenigen Inverkehrbringern aufgestellt sind, muss eine Vielzahl von einfach zu bedienenden, möglichst autonomen Verifikatoren 22 dort im Einsatz sein, wo auch immer solche Dokumente 1 einer Echtheitskontrolle unterzogen werden.

Die vom Hersteller angelieferten Dokumente 1 mit der Dokumentennummer 2 werden bei den Inverkehrbringern gelagert bis eines der Dokumente 1 einer berechtigten Person zugeteilt wird, wobei mittels des Validiergerätes 21 das dieser Person zugeteilte Dokument 1 durch Einschreiben der Kontrollnummer 9 in das Speicherfeld 4 zu einem Echtheitszertifikat 23 vervollständigt wird.

Eine Ausführung des Validiergeräts 21 gemäss Figur 6 umfasst eine Recheneinheit 24, eine Transportvorrichtung 25 für das Dokument 1, einen optischen Leser 26 zum maschinellen Auslesen der Kennung 7 (Figur 1) auf der optischen Markierung 3 des nicht aktivierten Dokuments 1 sowie ein Aufzeichnungsmittel 27. Weitere in der Zeichnung der Figur 6 gestrichelt eingezeichnete, fakultative Leseeinheiten 29 ermöglichen ein Ablesen der Dokumentennummer 2 (Figur 1), der Kontrollnummer 9 (Figur 2) und des Kodes 11 (Figur 2). Die Leseeinheiten 29 unterscheiden sich entsprechend der für das System 20 einmal gewählten Aufzeichnungstechniken, die für die Dokumentennummer 2, für die Kontrollnummer 9 und für den Kode 11 vorbestimmt sind. Die Transportvorrichtung 25, der optische Leser 26, das oder die Aufzeichnungsmittel 27 und die Leseeinheiten 29 sind mit der Recheneinheit 24 verbunden.

Die Recheneinheit 24 ist über Leitungen mit der Transportvorrichtung 25, dem optischen Leser 26, und mit dem Aufzeichnungsmittel 27 verbunden, steuert diese Geräte 25, 26, 27 und empfängt die von diesen Geräten 25, 26, 27 ausgesandte Informationen, damit das Dokument 1 maschinell abgelesen und beschriftet werden kann. Die Recheneinheit 24 weist wenigstens ein Sicherheitsmodul 30 auf, das in einer integrierte Schaltung einen Mikroprozessor mit zugehörigen Speicherplätzen umfasst. Der Mikroprozessor führt kryptographische Operationen aus und benutzt dazu den in den Speicherplätzen enthaltenen ersten geheimen Schlüssel 10.

Die Transportvorrichtung 25 bewirkt in einer Ausführung eine Relativbewegung zwischen dem Dokument 1 einerseits und den Lesemitteln 26, 29 und dem Aufzeichnungsmittel 27 andererseits. In der Figur 6 wird das Dokument 1 gegenüber den feststehenden Lesemitteln 26, 29 und dem Aufzeichnungsmittel 27 bewegt. Für die Transportvorrichtung 25 sind unterschiedliche, an sich bekannte Ausführungen für Blätter oder für Karten bekannt und einsetzbar. Auf eine aufwendige Transportvorrichtung 25 kann verzichtet werden, wenn die optische Markierung 3 bzw. das

Sicherheitselement 8 (Figur 1) gemäss der Lehre in der EP 0 883'085 A1 gestaltet ist und das Beschriften des Speicherfelds 4 manuell erfolgt.

Das Aufzeichnungsmittel 27 ist zum Einschreiben der Kontrollnummer 9 und des Kodes 11 in das Speicherfeld 4 bzw. Kodierfeld 5 eingerichtet und benutzt die für das Dokument 1 vorgesehene Aufzeichnungstechnik, beispielsweise ein Druck-, Tintenstrahl-, Xerographie-, Perforations- usw. Verfahren, ein in der EP 0 718 795 A1 beschriebenes Schreibverfahren für die Informationsträger 17, eine magnetische Aufzeichnung oder die elektronische Speicherung im Speicher 14 (Figur 3). Die Kontrollnummer 9 kann auch manuell in das Speicherfeld 4 mit dokumentechter Tinte eingeschrieben werden. Das Perforationsverfahren für Dokumente 1 ist z.B. im DE Gebrauchsmuster G 93 15 294.9 beschrieben.

Die Tastatur 28 ist ganz allgemein eine Eingabevorrichtung für aus Ziffern oder alphanumerische Zeichen bestehende Informationen. Die Eingabevorrichtung kann auch über einen Anschluss 28' an ein Telephon- oder Computernetzwerk 37 (Figur 5) mit dem Validiergerät 21 verbunden sein, insbesondere können die den Kode 11 bildenden Informationen von einer Zentralstelle abgerufen werden.

Die Leseeinheit 29 ist der für das Dokument 1 verwendeten Aufzeichnungstechnik angepasst. Die Leseeinheit 29 ist z.B. ein Klarschriftleser, ein Barkodeleser usw. für visuell lesbare Zeichen, aus denen sich die Dokumentennummer 2, die Kontrollnummer 9 und den Kode 11 zusammensetzen. Diese Leseeinheiten 29 tasten mit einem Lichtstrahl Teile oder das ganze Dokument 1 ab und messen die Intensität des vom Dokument 1 zurückgestreuten Lichts. Die für die magnetisch aufgezeichnete Informationen bzw. zum elektronischen Auslesen aus dem Speicher 14 geeignete Leseeinheit 29 ist allgemein bekannt.

Der Aufbau und Arbeitsweise des optischen Lesers 26 und für eine Leseeinheit 29, die zum Auslesen der Kontrollnummer 9 aus dem optischen Informationsträger 17 (Figur 4) befähigt ist, sind beispielsweise aus den eingangs genannten Schriften CH - PS 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1, EP 0 883'085 A1 bekannt.

In einer kostengünstigen Ausführung zur Aktivierung liest ein Bediensteter eines nicht aktivierten Dokuments 1 dessen Dokumentennummer 2 visuell ab und gibt die Dokumentennummer 2 (Figur 2) über eine Tastatur 28 manuell in die Recheneinheit 24 ein. Anschliessend wird das Dokument 1 in die auf einen Kanal oder eine Plattform reduzierte Transportvorrichtung 25 unter den optischen Leser 26 gesteckt bzw. gelegt, damit der optische Leser 26 die Kennung 7 ablesen und der Recheneinheit 24 übermitteln kann. Die Recheneinheit 24 verschlüsselt die Kennung 7 und die Dokumentennummer 2 mit dem ersten geheimen Schlüssels 10 und bildet eine digitale Signatur, die Kontrollnummer 9, auf einer Anzeige 31 ab. Der Bedienstete überträgt nun manuell die Kontrollnummer 9 in das Speicherfeld 4 auf dem Dokument 1, das nun derart aktiviert zum Echtheitszertifikat 23 (Figur 5) geworden ist. Das

Speicherfeld 4 kann in Felder für je ein Zeichen der Kontrollnummer 9 eingeteilt sein, um ein maschinelles Lesen der handschriftlich eingetragenen Kontrollnummer 9 zu erleichtern.

Eine zweite Ausführung weist eine in der Zeichnung der Figur 6 punktiert gezeichnete Lesereinheit 29 auf, die die Dokumentennummer 2 maschinell direkt vom Dokument 1 abliest und an die Recheneinheit 24 abgibt. Die Recheneinheit 24 verschlüsselt wenigstens die Kennung 7 und die Dokumentennummer 2 mit dem ersten geheimen Schlüssels 10 zur Kontrollnummer 9. Anschliessend überträgt das Aufzeichnungsmittel 27 die Kontrollnummer 9 in den Speicherfeld 4 in der vom System 20 vorbestimmten Technik.

Das Validiergerät 21 ist in einer dritten Ausführung zusätzlich mit der Tastatur 28 und der Anzeige 31 ausgestattet, um über die Tastatur 28 den Kode 11 einzugeben, wobei die Anzeige 31 zur Kontrolle des Kodes 11 dient. Der Kode 11 wird ebenfalls mit dem Aufzeichnungsmittel 27 auf das Dokument 1 übertragen. Für besonders wichtige Dokumente 1 ist das Validiergerät 21 dazu eingerichtet, die Eingabe einer persönlichen Identifikationsnummer (PIN) vom Benutzer zu verlangen. Diese PIN identifiziert in einem Fall als Zulassungs - PIN den Bediensteten, der das Validiergerät 21 bedient, und in einem zweiten Fall als Inhaber - PIN den Dokumentinhaber, wobei bei der Aktivierung des Dokuments 1 der Inhaber seine PIN über die Tastatur 28 eintippt und im Rechengerät 24 die Inhaber - PIN zusammen mit dem Kode 11 oder allein als Parameter für die Erzeugung der Kontrollnummer 9 dient.

In einer vierten Ausführung des Validiergeräts 21 ist anstelle des optischen Lesers 26 und der Leseeinheit 29 ein einziger Leser 26 so eingerichtet, dass er sowohl die optische Markierung 3 und die Dokumentennummer 9 erkennen kann.

In einer fünften Ausführung ist das Validiergerät 21 auch zum Erkennen der Kontrollnummer 9 eingerichtet. Somit ist das Validiergerät 21 fähig, aktivierte und nicht aktivierte Dokumente 1 zu unterscheiden und zusätzlich die Kontrollnummer 9 auf ihre Richtigkeit zu überprüfen.

Die Kontrollnummer 9 ist das Ergebnis der kryptographischen Operation in der Recheneinheit 24, einer mathematischen Funktion f:

Kontrollnummer 9 = f(Dokumentennummer 2, Kennung 7, erster geheimer Schlüssel 10) bzw.

Kontrollnummer 9 = f(Dokumentennummer 2, Kennung 7, Kode 11, erster geheimer Schlüssel 10).

Da sich die Systeme 20 nicht nur in der Aufzeichnungstechnik sondern auch in der Anzahl und Art der Parameter der kryptographischen Operation unterscheiden, werden, zwecks einfacherer Beschreibung, nachfolgend die für die Erzeugung der Kontrollnummer 9 auf dem Dokument 1 vorhandenen Werte, wie Dokumentennummer 2, Kennung 7, Kode 11 und die getrennt vom Dokument 1 gespeicherte Inhaber - PIN, als Parameter der kryptographischen Operation bezeichnet, wobei darunter wenigstens die Dokumentennummer 2 und die Kennung 7 zu verstehen sind, allenfalls ergänzt um den Kode 11

und/oder die Inhaber - PIN. Ein System 20 ist somit durch die verwendeten Aufzeichnungstechniken, die Ausführung des Dokuments 1, die Parameter der kryptographischen Operation und dem ersten geheimen Schlüssel 10 bestimmt.

Weder der erste geheime Schlüssel 10 noch der Algorithmus sind der Öffentlichkeit bekannt und werden von einer "certification authority" in einem Sicherheitmodul 30 zum Einsetzen in die Recheneinheit 23 abgegeben. Nachdem die Recheneinheit 24 die Parameter der Funktion f in das Sicherheitsmodul 30 eingegeben sind, erzeugt das leicht auswechselbare Sicherheitsmodul 30 direkt die Kontrollnummer 9 oder ein Zwischenresultat, das für die Berechnung der Kontrollnummer 9 in der Recheneinheit 24 dient.

Der erste geheime Schlüssel 10 dient sowohl für die kryptographischen Operation zum Erzeugen der Kontrollnummer 9 als auch für die Überprüfung der Richtigkeit der Kontrollnummer 9 in Kenntnis der auf dem Dokument 1 vorhandenen Informationen.

Der Verifikator 22 in der Figur 7 weist bis auf das Aufzeichnungsmittel 27 (Figur 6) gleiche Komponenten wie das Validiergerät 21 (Figur 6) auf. Die Ausführungen des Verifikator 22 unterscheiden sich in den Leseeinheiten 29, die sich entsprechend der für das System 20 (Figur 5) gewählten Aufzeichnungstechnik unterscheiden. Der Verifikator 22 umfasst in der kostengünstigen Ausführung wenigstens ein Aufnahmemittel 32 für ein zu überprüfendes Echtheitzertifikat 23 (Figur 5), ein Rechengerät 33 mit dem Sicherheitsmodul 30, den optischen Leser 26 für die Kennung 7, die Tastatur 28 und die Anzeige 31. Das Rechengerät 33 ist mit dem optischen Leser 26, der Tastatur 28 und der Anzeige 31 verbunden. Das Rechengerät 33 überprüft mit einer anderen kryptographischen Operation, ob die Kontrollnummer 9 (Figur 2) zu den Parametern der kryptographischen Operation, die wenigstens die Dokumentnummer 2 und die Kennung 7 umfassen, passt. Dazu verwendet das Rechengerät 33 einen zweiten Schlüssel 34, der im Sicherheitsmodul 30 mit dem entsprechenden Algorithmus enthalten ist. Das Rechengerät 33 kann mit der anderen kryptographischen Operation keine Verschlüsselungen wie die Recheneinheit 24 (Figur 6) im Validiergerät 21 vornehmen. Die Verwendung des zweiten Schlüssels 34, der vom ersten Schlüssel 10 völlig verschieden ist, weist den Vorteil auf, dass die sich aus der Verwendung ergebenden weiten Verbreitung der Verifikatoren 22 ergebenden Schwierigkeit der Geheimhaltung des zweiten Schlüssels 34 für die Sicherheit des Systems 20 irrelevant ist. Das Rechengerät 32 stellt das Ergebnis der Echtheitskontrolle auf der Anzeige 31 dar.

Für eine Echtheitskontrolle liest ein Kontrolleur visuell die Parameter der kryptographischen Operation, wenigstens die Dokumentnummer 2 und die Kennung 7, auf dem Echtheitszertifikat 23 und die Kontrollnummer 9 im Speicherfeld 4 ab und führt dem Rechengerät 33 die abgelesenen Zeichenfolgen über die Tastatur 28 zu. Das Aufnahmemittel 32 kann auch eine einfache Plattform unter dem optischen Leser 26 sein, auf die der Kontrolleur das Dokument 1 so auflegt, dass die optische Markierung 3 im

Bereich des optischen Lesers 26 ist. Die maschinell gelesene Kennung 7 gelangt direkt in das Rechengerät 33. Das Ergebnis der Echtheitskontrolle erscheint auf der Anzeige 31. Im einfachsten Fall besteht die Anzeige 31 aus zwei Signallampen um das Ja/Nein - Ergebnis der Echtheitskontrolle darzustellen. Jedoch ist es von Vorteil, wenn die Anzeige 31 sowohl die über die Tastatur 28 eingegebenen Parameter und Kontrollzahl 9 sowie das Ja/Nein - Ergebnis anzeigt.

Der Verifikator 22 gibt in einer anderen Ausführung ein Erlaubnissignal über eine Signalleitung 35 an eine Dienstleistungseinrichtung 36 ab. Das Eintreffen des Erlaubnissignals gibt die Dienstleistung der Dienstleistungseinrichtung 36 frei, z.B. Türöffnung, Geldausgabe, Warenbezug, Registrierung usw.

Eine andere Ausführung des Verifikators 22 weist als Aufnahmemittel 32 ein Transportsystem für blatt- oder kartenförmige Dokumente 1 auf. Mit dem Rechengerät 33 ist das vom Rechengerät 33 gesteuerte Aufnahmemittel 32 und zusätzlich zum optischen Leser 26 wenigstens eine Leseeinheit 29 zum Übermitteln von Informationen verbunden. Die Leseeinheit 29 liest einen oder mehrere Parameter der kryptographischen Operation maschinell aus. Eine Tastatur 28 erübrigt sich für diese Ausführung. Eine Leseeinheit 29 ist dann ausreichend, wenn die Parameter der kryptographischen Operation und die Kontrollnummer 9 auf dem Echtheitszertifikat 23 in der gleichen Aufzeichnungstechnik ausgeführt sind.

Für ein System 20, bei dem der Inhaber - PIN verwendet wird, ist die Tastatur 28 für den Inhaber vorgesehen, der sich mit der Inhaber - PIN gegenüber dem Verifikator 22 identifiziert. Die über die Tastatur eingegebene Inhaber - PIN wird in der kryptographischen Operation als Parameter zur Überprüfung der Kontrollnummer 9 verwendet.

Wie beim Validiergerät 21 ist auch eine Identifizierung des Kontrolleurs mittels seiner Benutzer - PIN von Vorteil, um die Hürde für potentielle Einbrecher in das System 20 möglichst hoch anzusetzen. Die Eingabe der richtigen Benutzer - PIN über die Tastatur 28 ermöglicht dem Rechengerät 33 den Benutzer zu identifizieren und den Validator 22 zum Einsatz freizugeben.

Zur Figur 5 ist noch zu bemerken, dass das System 20 mit Vorteil in ein bidirektionales Telephon- oder Computernetzwerk 37 zum Datenaustausch zwischen den Validiergeräten 21 und den Verifikatoren 22 einerseits und einem Rechner 37 andererseits eingebettet ist. Das Validiergerät 21 ist über den Anschluss 28' mit dem Netzwerk 37 und das Netzwerk 37 über eine Leitung 38 mit dem zentralen Rechner 39 verbunden. Neben dem bereits erwähnten Abruf von Daten aus dem zentralen Rechner 39 für den Kode 11 (Figur 2) ermöglicht das Netzwerk 37 im zentralen Rechner 39 eine Negativliste Dokumentennummern 2 von widerrufenen Echtheitszertifikaten 23 anzulegen. Die über das Netzwerk 37 mit dem zentralen Rechner 39 verbundenen Verifikatoren 22 erhalten über eine Datenleitung 40 die regelmässig nachgeführte Negativliste in das Rechengerät 33 (Figur 7) übertragen. Die Negativliste ist in einem Datenspeicher 41 (Figur 7) des Rechengeräts 33 abgelegt, damit auch beim

Ausfall des Netzwerkes 37 widerrufene Echtheitszertifikate 23 von den Verifikatoren 22 erkannt werden.

PATENTANSPRÜCHE

1. Dokument (1) mit einer wenigstens maschinell lesbaren Dokumentennummer (2) auf dem Substrat (6) und einem Speicherfeld (4) für die Aufnahme einer Kontrollnummer (9) dadurch gekennzeichnet, dass auf dem Substrat (6) eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) angebracht ist, dass das Speicherfeld (4) zur Aufnahme der wenigstens maschinell lesbaren Kontrollnummer (9) eingerichtet ist und dass die Kontrollnummer (9), die das Ergebnis einer kryptographischen Operation mit wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), und einem ersten geheimen Schlüssel (10) ist, zur Vervollständigung erst bei der Inverkehrbringung als Echtheitszertifikats (23) im Speicherfeld (4) eingesetzt ist.

2. Dokument (1) nach Anspruch 1, dadurch gekennzeichnet, dass die optische Markierung (3) beugungsoptische Strukturen aufweist und dass wenigstens ein Teil der beugungsoptischen Strukturen die maschinell lesbare Kennung (7) enthält.

3. Dokument (1) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Substrat (6) ein Kontrollfeld (5) für die Aufnahme eines wenigstens visuell lesbaren, individuellen und auf eine Person bezogenen Kodes (11) aufweist.

4. Dokument nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, dass das Speicherfeld (4) auf dem Substrat (6) angeordnet ist und dass nach der Aktivierung die Kontrollnummer (9) im Speicherfeld (4) in wenigstens maschinell lesbaren Zeichen enthalten ist.

5. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass im Substrat (6) ein Mikrochip (13) eingelassen ist, dass das Speicherfeld (4) im Speicher (14) des Mikrochips (13) angeordnet ist und dass nach der Aktivierung das Speicherfeld (4) die Kontrollnummer (9) enthält und der einmal eingeschriebene Inhalt des Speicherfelds (4) elektronisch nicht veränderbar ist.

6. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein Magnetstreifen (16) mit dem Speicherfeld (4) angeordnet ist, dass der Magnetstreifen (16) wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung das Speicherfeld (4) die magnetisch lesbare Kontrollnummer (9) aufweist.

7. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein optischer Informationsträger (17, 17') angeordnet ist, dass der optische Informationsträger (17, 17') wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung der nicht mehr veränderbare optische Informationsträger (17, 17'') im Speicherfeld (4) die Kontrollnummer (9) in optisch lesbaren Zeichen aufweist.

8. Dokument (1) nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass ein Teil des optischen Informationsträgers (17, 17') die optische Markierung (3) bildet und die Kennung (7) enthält.

9. System (20) bestehend aus wenigstens einem Dokument (1) nach einem der Ansprüche 1 bis 8, einem Validiergerät (21) und einem Verifikator (22), dadurch gekennzeichnet, dass das Dokument (1) wenigstens eine maschinell lesbare Dokumentennummer (2), eine optische Markierung (3) mit einer maschinell lesbare Kennung (7) und ein wenigstens maschinell lesbares Speicherfeld (4) für die Aufnahme einer Kontrollnummer (9) aufweist,
dass im Validiergerät (21) eine Aufnahmevorrichtung (25) zur Aufnahme des Dokuments (1) und einen optischen Leser (26) zum maschinellen Ablesen von wenigstens der Kennung (7) angeordnet sind, dass im Validiergerät (21) eine Recheneinheit (24) für kryptographische Operationen mit einem ersten geheimen Schlüssel (10) zum Erzeugen der Kontrollnummer (9) durch Verschlüsseln von wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), vorhanden ist, dass ein Aufzeichnungsmittel (27) zum Einschreiben der Kontrollnummer (9) in das wenigstens maschinell lesbare Speicherfeld (4) eingerichtet ist,
dass der Verifikator (22) wenigstens ein Rechengerät (33), einen optischen Leser (26) zum maschinellen Ablesen der Kennung (7) und ein Aufnahmemittel (32) zum Ausrichten eines Echtheitszertifikats (23) zum maschinellen Ablesen aufweist, dass der Verifikator (22) das wenigstens mit Eingabe- und Ablesemitteln (26; 28; 29) verbundene Rechengerät (33) für kryptographische Operationen mit einem zweiten Schlüssel (34) enthält und dass das Rechengerät (33) zur Überprüfung der Zusammengehörigkeit wenigstens der Kontrollnummer (9) und den zum Verschlüsseln benutzten Parametern der kryptographischen Operation, die auf dem Echtheitszertifikat (23) enthalten sind, und zur Darstellung des Vergleichsergebnisses auf einer Anzeige (31) des Verifikators (22) und/oder zur Erzeugung eines Erlaubnissignals eingerichtet ist.

10. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass der Verifikator (22) eine Tastatur (28) für eine manuelle Eingabe einer persönlichen Identifikationsnummer (PIN) zur Freigabe des Verifikators (22) aufweist und dass der Verifikator (22) zum Überprüfen der persönlichen Identifikationsnummer eingerichtet ist.

11. System (20) nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass der Verifikator (22) eine mit dem Rechengerät (33) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) und der Kontrollnummer (9) an das Rechengerät (33) aufweist.

12. System (20) nach einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, dass der Verifikator (22) wenigstens eine mit dem Rechengerät (33) verbundene Leseeinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) und der Kontrollnummer (9) an das Rechengerät (33) aufweist.

13. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) an die Recheneinheit (24) aufweist.

14. System (20) nach Anspruch 9 oder 13, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Leseeinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) an die Recheneinheit (24) aufweist.

15. System (20) nach Anspruch 9, 13 oder 14, dadurch gekennzeichnet, dass das Validiergerät (21) für die Eingabe eines individuellen, auf eine Person bezogenen Kodes (11) mittels der Tastatur (28) eingerichtet ist und, dass das Aufzeichnungsmittel (27) im Validiergerät (21) zum Einschreiben des Kodes (11) in das Kontrollfeld (5) angeordnet ist.

16. System (20) nach einem der Ansprüche 9 bis 15, dadurch gekennzeichnet, dass die Recheneinheit (24) im Validiergerät (21) derart ausgebildet ist, dass bei der Verschlüsselung der Kontrollnummer (9) eine über eine Tastatur (28) eingegebene persönlichen Identifikationsnummer Nummer der berechtigten Person als Parameter für die Erzeugung der Kontrollnummer (9) einbezogen ist und dass der Verifikator (22) das Erlaubnissignal nur dann im Rechengerät (33) erzeugt, wenn bei der Echtheitsprüfung die persönlichen Identifikationsnummer Nummer über die Tastatur (28) des Verifikators (22) dem Rechengerät (33) als Parameter der kryptographischen Operation einbezogen ist.

17. System (20) nach einem der Ansprüche 9 bis 16, dadurch gekennzeichnet, dass wenigstens ein Validiergerät (21) und wenigstens ein Verifikator (22) über ein Netzwerk (28', 38, 40; 37) mit einem zentralen Rechner (39) zum bidirektionalen Datenaustausch verbunden sind.

18. System (20) nach einem der Ansprüche 9 bis 17, dadurch gekennzeichnet, dass das wenigstens ein Verifikator (22) über eine Signalleitung (35) mit einer Dienstleistungseinrichtung (36) verbunden ist und dass die Dienstleistungseinrichtung (36) zum Freigeben einer Dienstleistung mittels des über die Signalleitung (35) an die Dienstleistungseinrichtung (36) gesandten Erlaubnissignals eingerichtet ist.

ZUSAMMENFASSUNG

Ein Dokument (1) weist auf dem Substrat (6) wenigstens eine Dokumentennummer (2), eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) und ein Speicherfeld (4) für die Aufnahme einer Kontrollnummer (9) auf. Die Kontrollnummer (9) wird erst im Moment der Abgabe an eine berechtigte Person mittels einer kryptographischen Operation aus wenigstens der Dokumentennummer (2), der Kennung (7) und einem ersten geheimen Schlüssel (10) erzeugt und in das Speicherfeld (4) eingeschrieben. Ein derart erzeugtes Echtheitszertifikat ist mit einem Verifikator unter Verwendung einer kryptographischen Operation und der auf dem Dokument (1) gespeicherten Information mittels eines zweiten Schlüssels auf seine Echtheit überprüfbar.

(Fig. 2)

Fig. 1:

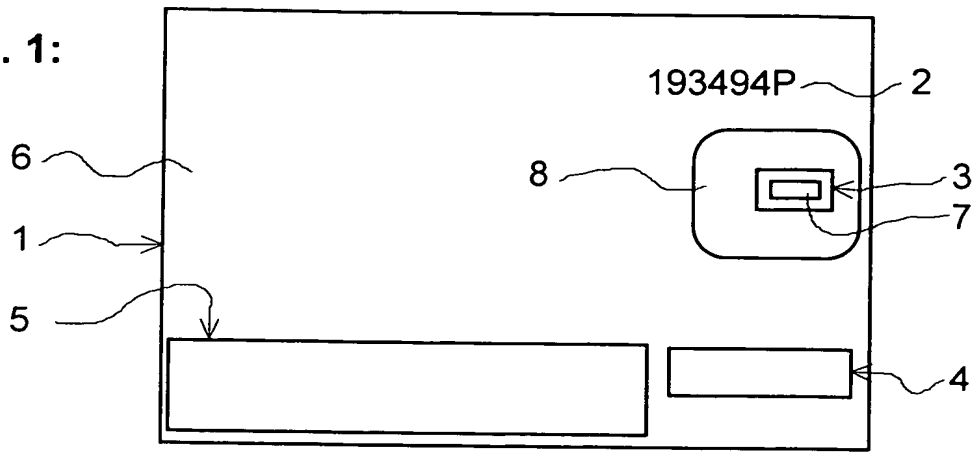


Fig. 2:

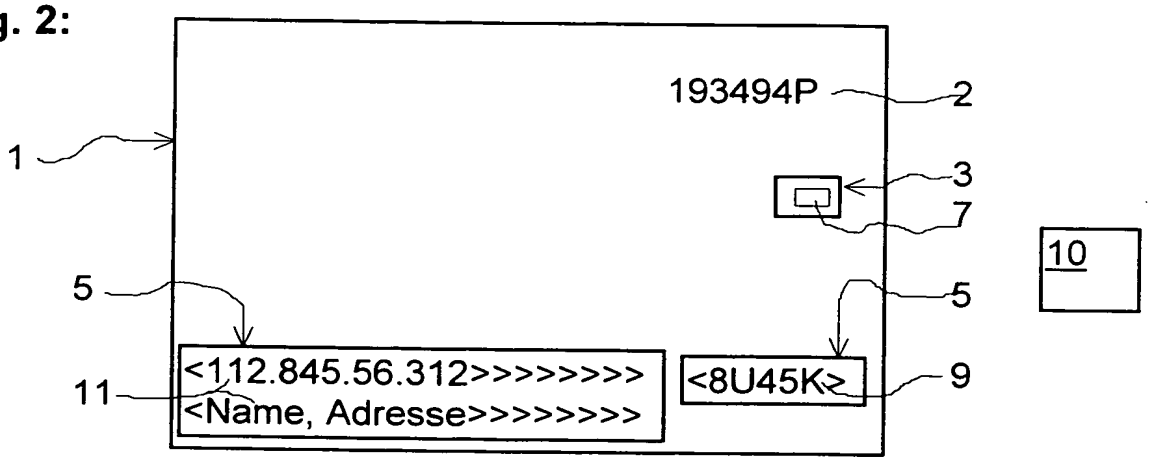


Fig. 3:

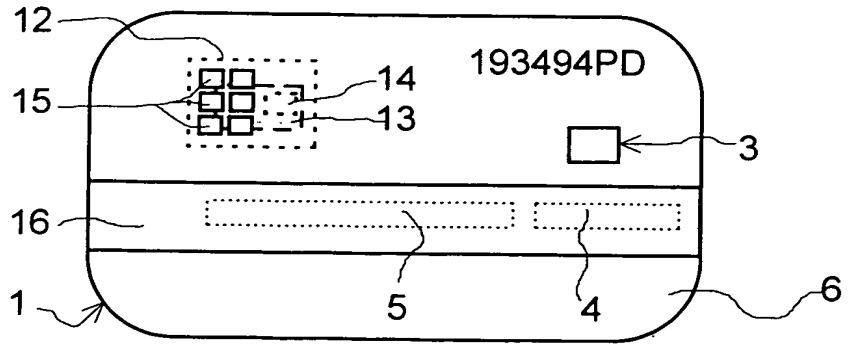


Fig. 4:

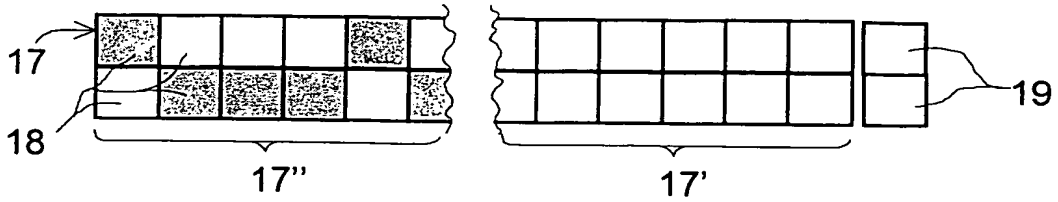


Fig. 5:

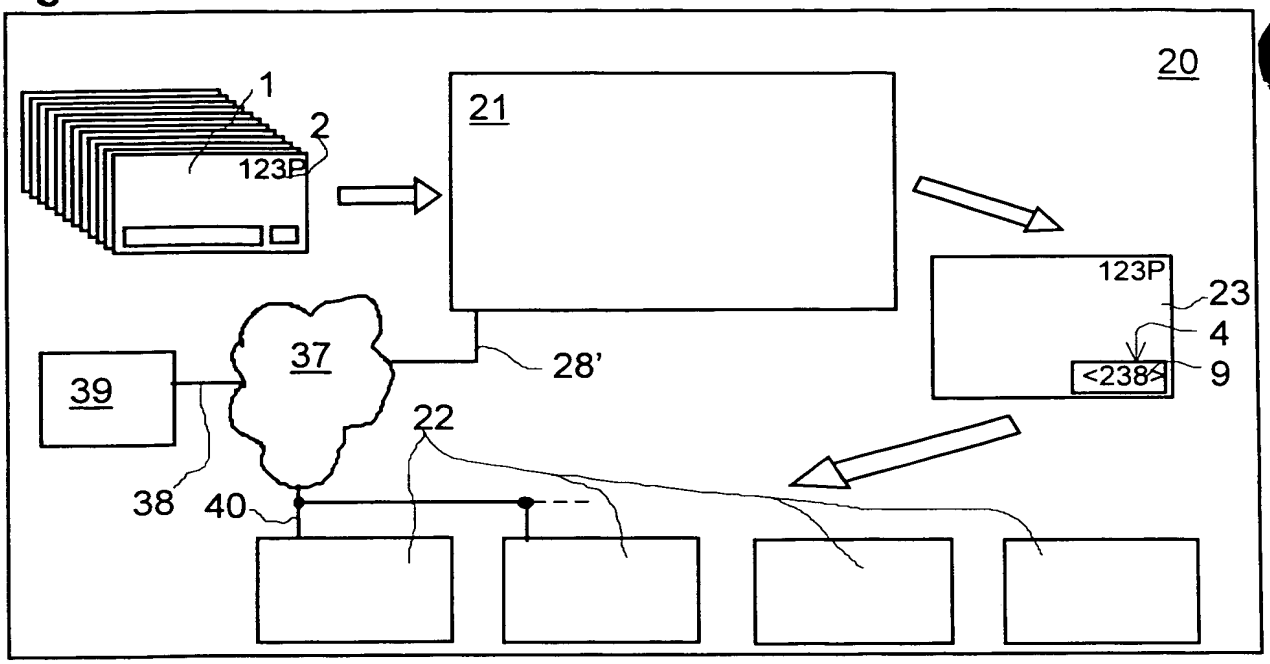


Fig. 6:

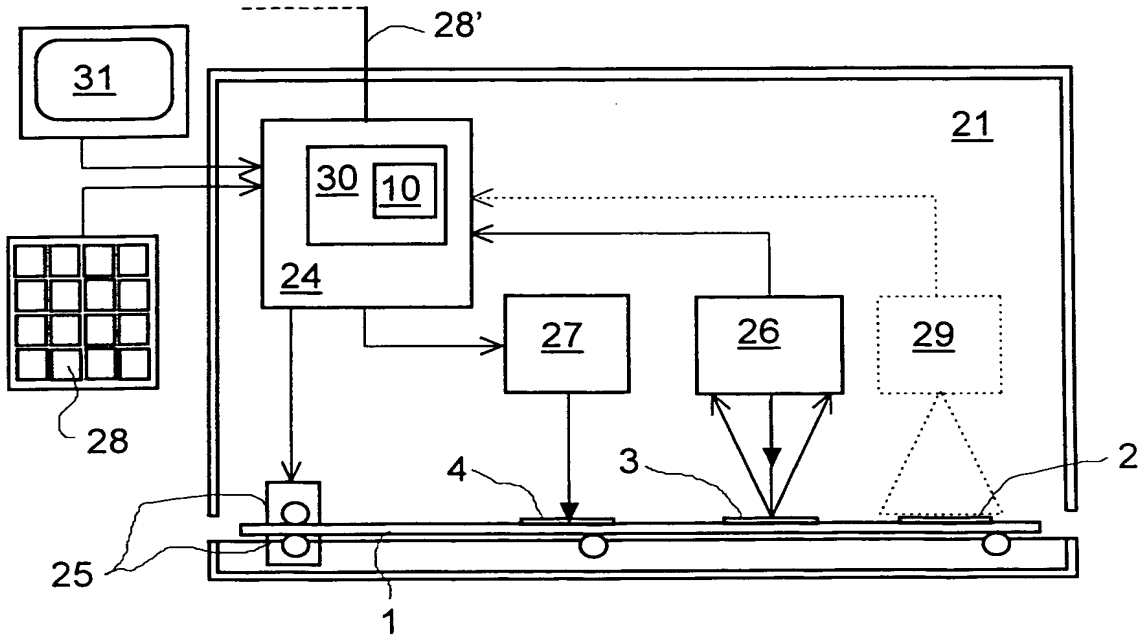


Fig. 7: